UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

KELLY ABRAMOWITZ, individually and on behalf of all others similarly situated, Plaintiff, v. UNITED HEALTHCARE SERVICES, INC. d/b/a UNITEDHEALTHCARE STUDENT RESOURCES Defendant.	**Case No.** **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Kelly Abramowitz ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this class action complaint against Defendant UnitedHealthcare Services, Inc. d/b/a UnitedHealthcare Student Resources, ("UnitedHealthcare" or "Defendant"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action lawsuit on behalf of all persons who entrusted UnitedHealthcare with sensitive personal information that was subsequently exposed in a data breach (the "Data Breach" or the "Breach").[1]

2. Plaintiff's claims arise from UnitedHealthcare 's failure to safeguard personally identifying information ("PII") and protected health information ("PHI") that was entrusted to it

[1] *Submitted Breach Notification Sample: UnitedHealthcare Student Resources*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL https://oag.ca.gov/ecrime/databreach/reports/sb24-570667 (last visited August 30, 2023).

in its capacity as a health insurance company. On May 27, 2023, hackers accessed UnitedHealthcare's file transfer servers which contained its customers' sensitive PII and PHI.[2]

3. UnitedHealthcare is "the largest single health carrier in the United States" and provides insurance services to "both domestic and international students[.]"[3] United Healthcare Student Resources is a health benefits business and does business under UnitedHealthcare, an operating division of UnitedHealth Group ("UnitedHealth") which offers a range of "health benefit plans[.]"[4]

4. As part of its services, UnitedHealthcare provides the PII and PHI of its past and current customers to Progress Software Corporation ("PSC") in connection with the audit and other services offered by PSC.

5. PSC owns and operates the MOVEit, a file sharing application that they created, to ostensibly securely transmit files or to allow other companies to do so. On or about May 31, 2023, PSC was alerted that an unauthorized external party had exploited a vulnerability within the MOVEit software. PSC then initiated an inquiry and determined that this unauthorized party had gained entry to one of PSC's MOVEit Transfer servers on May 27, 2023. During this breach, the unauthorized party acquired data containing sensitive personal PII and PHI of both UnitedHealthcare clientele, including the Plaintiff and other members of the class was impacted.

6. To access insurance and/or services from UnitedHealthcare, the Plaintiff and members of the Class furnished sensitive and private PII and PHI to UnitedHealthcare, including their names, dates of birth, address, phone number, email addresses, plan identification number, policy information, student identification number, and claim information, including diagnosis

[2] *Id*.
[3] *About Us*, UNITEDHEALTHCARE STUDENT RESOURCES https://www.uhcsr.com/about-us (last visited August 30, 2023).
[4] *Id*.

codes, prescription information, and financial information associated with claims.

7. Defendant made promises and representations to Plaintiff and the class she seeks to represent that the PII and PHI collected as part of providing those services would be kept safe, confidential, and maintained by Defendant, and that Defendant would delete any sensitive information regarding Plaintiff once that information was no longer needed.

8. Despite acting and marketing itself as a safe container for sensitive information, UnitedHealthcare failed to take precautions designed to keep that information secure.

9. The data that United Healthcare exposed was highly sensitive, including names, addresses, dates of birth, and various aspects of the claim information, including diagnosis codes and financial information associated with United Healthcare members' claims. The compromised data also allows individuals to know that consumers used or considered use of an UnitedHealthcare product, including health insurance policy information, potentially disclosing health conditions.

10. UnitedHealthcare acknowledges that information in its system was accessed by unauthorized individuals. The Data Breach affecting UnitedHealthcare was part of a much larger data breach surrounding the MOVEit software that impacted more than 600 organizations and nearly 40 million people worldwide so far.[5]

11. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, substantiates that Plaintiff and Class members have suffered irreparable harm. Plaintiff and Class members have lost the ability to control their private information and are subject to an increased risk of identity theft.

[5] Raphael Satter & Zeba Siddiqui, *Analysis: MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts*, REUTERS https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/ (last visited August 31, 2023).

12. Defendant owes a duty to Plaintiff and Class members to maintain adequate security measures to safeguard the PII and PHI it requested and was entrusted with. Defendant breached its duty by failing to implement and/or maintain adequate security practices. The PHI disclosed here is also protected under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

13. UnitedHealthcare delayed acknowledging and giving notice of the Data Breach. UnitedHealthcare did not notify its customers of the data breach until after its investigation concluded July 27, 2023 (the "Notice Letter"). Defendant waited to alert Plaintiff and Class Members, despite knowing that hackers accessed its account holders and customers information, that sensitive PII and PHI was compromised.

14. As a result of the UnitedHealthcare's inadequate digital security and notice process, Plaintiff and Class members' PII and PHI was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries, including: financial losses caused by misuse of their PII; the loss or diminished value of their PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal, medical, and financial information.

15. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence per se; breach of implied contract; and unjust enrichment.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

18. Plaintiff Kelly Abramowitz is a citizen of Philadelphia, Pennsylvania. Plaintiff Abramowitz received the Notice Letter via email on or about July 27, 2023, notifying her that her information was part of the Data Breach. In or around July 11, 2023, Plaintiff Abramowitz experienced unusual activity in the form of a fraudulent charge on her credit card, which required her to cancel and then reorder a new credit card. Plaintiff Abramowitz has further experienced an increase in spam emails in the past several months.

19. Defendant United HealthCare Services, Inc. d/b/a UnitedHealthcare Student Resources is a Minnesota corporation with its principal place of business located at 9900 Bren Road East, Minnetonka, Minnesota 55343.

FACTUAL BACKGROUND

A. The Data Breach

20. On or about July 27, 2023, UnitedHealthcare began sending Plaintiff and other Class members a Notice of Data Breach letter (the "Notice Letter") notifying them that they were the subject of a Data Breach in connection with the MOVEit software. The Notice Letter indicated that highly sensitive personal information of its customers was compromised in the Data Breach, including names, dates of birth, address, phone number, email addresses, plan identification number, policy information, student identification number, and claim information, including diagnosis codes, prescription information, and financial information associated with claims.

21. UnitedHealthcare, or an entity UnitedHealthcare entrusts with their data, employs software named MOVEit, which is supplied by PSC. MOVEit's intended use is to safely move files as part of their routine operations. Within this process, UnitedHealthcare uploads, retains,

shifts, or retrieves PII and PHI owned by UnitedHealthcare clients. This data is shared with UnitedHealthcare and managed using the MOVEit software.

22. On or about May 31, 2023, PSC announced that it discovered a vulnerability in the MOVEIT software that was exploited by an unauthorized third party.

23. UnitedHealthcare reportedly performed an internal investigation into the scope of the vulnerability in MOVEit's software and the impacted on their systems.[6] UnitedHealthcare's investigation revealed that the third party accessed one of their MOVEit servers on May 27, 2023 and the third party downloaded data from its servers.[7] UnitedHealthcare conducted a manual review of their records was completed on June 12, 2023, and confirmed the identities of individuals affected by the breach.

24. While UnitedHealthcare sought to minimize the damage caused by the breach, it cannot and has not denied that there was unauthorized access to the PII and PHI of Plaintiff and Class members.

25. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

26. Plaintiff and Class members were or are UnitedHealthcare customers or account holders that entrust UnitedHealthcare with their PII and PHI.

B. UnitedHealthcare's Obligation to Protect Plaintiff and Class members' PII

27. UnitedHealthcare Student Resources provides health insurance services to students through UnitedHealthcare. UnitedHealthcare provides health insurance coverage to 27

[6] *UnitedHealthcare Student Resources Notifies Individuals of Data Security Incident*, UNITEDHEALTHCARE STUDENT RESOURCES https://www.uhcsr.com/media/dbd8af76-4e09-4bd1-b94c-eb94a4b4fdc6 (last visited August 31, 2023).
[7] *Id*.

million people as individuals, through employers, or otherwise.[8]

28. UnitedHealthcare and its related entities annual revenue was $324.2 billion for the 2022 financial year.[9]

29. UnitedHealthcare Privacy Policy highlights its protection of PII and PHI, stating that:

> We are required by law to protect the privacy of your health information. We are also required to send you this notice, which explains how we may use information about you and when we can give out or "disclose" that information to others. You also have rights regarding your health information that are described in this notice. We are required by law to abide by the terms of this notice.
>
> The terms "information" or "health information" in this notice include any information we maintain that reasonably can be used to identify you and that relates to your physical or mental health condition, the provision of health care to you, or the payment for such health care. We will comply with the requirements of applicable privacy laws related to notifying you in the event of a breach of your health information.
>
> * * *
>
> We do not disclose personal financial information about our enrollees or former enrollees to any third party, except as required or permitted by law. [10]

C. UnitedHealthcare's Failure to Prevent, Identify and Timely Report the Breach

30. UnitedHealthcare failed to take adequate measures to protect its computer systems and internal network against unauthorized access.

31. UnitedHealthcare was not only aware of the importance of protecting the PII and PHI that it maintains, as alleged, it touted its capability to do so. The PII and PHI UnitedHealthcare allowed to be exposed in the Data Breach is the type of private information that

[8] *Our Businesses*, UNITEDHEALTH GROUP https://www.unitedhealthgroup.com/people-and-businesses/businesses/unitedhealthcare.html (last visited August 31, 2023).
[9] *Earnings Reports & SEC Filings: Q4 2022*, UNITEDHEALTH GROUP https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2022/UNH-Q4-2022-Release.pdf (last visited August 31, 2023).
[10] *UnitedHealthcare® Student Resources Health Plan Notices of Privacy Practices*, UNITEDHEALTHCARE https://www.uhc.com/content/dam/uhcdotcom/en/npp/NPP-UHC-StudentResources-EN.pdf (last visited August 31, 2023).

UnitedHealthcare knew or should have known would be the target of cyberattacks.

32. Despite its own knowledge and supposed expertise on the subject of cybersecurity, notwithstanding the FTC's data security principles and practices,[11] UnitedHealthcare failed to disclose that its systems and security practices were inadequate to reasonably safeguard sensitive personal information.

33. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[12] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves. Despite this guidance, UnitedHealthcare delayed the notification of the Data Breach.

D. The Harm Caused by the Data Breach, Now and Going Forward

34. Victims of data breaches are susceptible to becoming victims of identity theft.

35. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[13]

36. The type of data that was accessed and compromised here can be used to perpetrate fraud and identity theft.

37. Plaintiff and Class members face a substantial risk of identity theft given that their

[11] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited August 31, 2023).
[12] *Id.*
[13] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited August 31, 2023).

names, student identification numbers, addresses, dates of birth, and heath claim information were compromised.

38. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

39. When malicious actors infiltrate companies and copy and exfiltrate the PII and PHI that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[14]

40. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[15]

41. PII and PHI remain of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank

[14] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited August 31, 2023).

[15] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited August 31, 2023).

details have a price range of $50 to $200.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

42. The PII and PHI compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[18]

43. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[19]

44. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[20] Defendant did not rapidly or timely report to Plaintiff and Class members that their PII and PHI had been stolen. UnitedHealthcare, however, delayed notification of the compromise.

45. UnitedHealthcare offered victims unspecified "free identity theft protection service[s] . . ." The service offered by UnitedHealthcare is inadequate. Identity thieves often hold onto personal information in order to commit fraud years after such free programs expire.[21]

---

[16] *Id.*
[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 31, 2023).
[18] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited August 31, 2023).
[19] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (last visited August 31, 2023).
[20] *Id.*
[21] Scott Steinberg, *The latest ways identity thieves are targeting you — and what to do if you are a victim*, CNBC (Feb. 27, 2020) https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html (last visited August 31, 2023).

46. As a result of the Data Breach, Plaintiff and Class members' PII and PHI has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII and PHI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII and PHI;

e. Improper disclosure of their PII and PHI;

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII and PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and PHI being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of obtaining medical insurance services from Defendant; and the loss of Plaintiff's and Class members' privacy.

47. In addition to a remedy for economic harm, Plaintiff and Class members maintain an interest in ensuring that their PII and PHI is secure, remains secure, and is not subject to further misappropriation and theft.

48. Defendant disregarded the rights of Plaintiff and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

49. The actual and adverse effects to Plaintiff and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Class:

> All persons in the United States whose personal information was compromised in the data breach publicly announced by UnitedHealthcare on or around July 27, 2023 (the "Class").

51. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

52. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

53. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

54. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiff estimates that the Class is comprised of at least one million Class members. The Class is sufficiently numerous to warrant certification.

55. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class members because they all had their PII and PHI compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the

Class. The harm suffered by Plaintiff is similar to that suffered by all other Class members that was caused by the same misconduct by Defendant.

56. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interest antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

57. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

58. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Class Member's PII and PHI was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class members' PII and PHI;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class members' privacy;

g. Whether Defendant took sufficient steps to secure its customers' PII and PHI;

h. Whether Defendant was unjustly enriched;

i. The nature of relief, including damages and equitable relief, to which Plaintiff and members of the Class are entitled.

59. Information concerning Defendant's policies is available from Defendant's records.

60. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

61. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

62. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

63. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

64. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

65. Plaintiff brings this claim individually and on behalf of the Class members.

66. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

67. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class members' PII and PHI.

68. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

69. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' PII and PHI.

70. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

71. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations, such as HIPAA, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

72. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI.

73. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII and PHI;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to adequately and timely notify impacted consumers of the Data Breach; and

e. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

74. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' PII and PHI within Defendant's possession.

75. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class members' PII and PHI.

76. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class members that the PII and PHI within Defendant's possession might have been compromised and precisely the type of information compromised.

77. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class members' PII and PHI would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

78. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class members' PII and PHI would result in injuries to Plaintiff and Class members.

79. Defendant's breach of duties owed to Plaintiff and Class members caused Plaintiff's and Class members' PII and PHI to be compromised.

80. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII and PHI would not have been compromised.

81. As a result of Defendant's failure to timely notify Plaintiff and Class members that their PII and PHI had been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

82. As a result of Defendant's negligence and breach of duties, Plaintiff and Class members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class or Alternatively the Wisconsin Subclass)

83. Plaintiff re-alleges and incorporates by reference herein all the allegations contained above.

84. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by UnitedHealthcare of failing to use reasonable measures to protect Plaintiff's and Class members' Private Information. Various FTC publications and orders also form the basis of UnitedHealthcare's duty.

85. UnitedHealthcare violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class members' PII and PHI, and not complying with industry standards.

86. UnitedHealthcare's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on UnitedHealthcare's systems.

87. UnitedHealthcare's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

88. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

89. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

90. As a result of Defendant's negligence, Plaintiff and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

91. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

92. Plaintiff and the Class provided and entrusted their PII and PHI to Defendant. Plaintiff and the Class provided their PII and PHI to Defendant, as part of Defendant's regular business practices.

93. UnitedHealthcare should have been aware that it had a minimum duty to alert Plaintiff and Class members that their data was compromised "without unreasonable delay."

94. Thus, when Defendant took Plaintiff's and Class members' PII and PHI, it entered into implied contracts with Plaintiff and Class members by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the PII and PHI of Plaintiff and Class members in its possession was secure.

95. Pursuant to these implied contracts, Plaintiff and Class members provided Defendant with their PII and PHI in order for Defendant to provide their services, for which

Defendant is compensated. In exchange, Plaintiff understood, and Defendant agreed to, among other things, that Defendant would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII and PHI; (3) protect Plaintiff's and Class members PII and PHI in compliance with federal and state laws and regulations and industry standards; and (4) notify Plaintiff and Class members in compliance with state laws and regulations.

96. Implied in these exchanges was a promise by Defendant to ensure the PII and PHI of Plaintiff and Class members in its possession was only used to provide the agreed-upon reasons, that Defendant would take adequate measures to protect Plaintiff's and Class members' PII and PHI, and that Defendant would notify Plaintiff and Class members where data safeguards failed.

97. A material term of this contract is a covenant by Defendant that they would take reasonable efforts to adequately secure that information. Defendant breached this covenant by allowing Plaintiff's and Class members' PII and PHI to be accessed in the Data Breach.

98. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information securely and respond accordingly if that information was compromised.

99. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII and PHI in exchange for services by Defendant. These agreements were made by Plaintiff and Class members as Defendant's customers.

100. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class members would not have disclosed their PII and PHI to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have obtained

Plaintiff's and Class members' PII if it did not intend to provide Plaintiff and Class members with its services.

101. Defendant was therefore required to reasonably safeguard and protect the PII and PHI of Plaintiff and Class members from unauthorized disclosure and/or use and, as promptly as reasonable, notify Plaintiff and Class members when it failed in that duty.

102. Plaintiff and Class members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

103. Plaintiff and Class members would not have entrusted their PII and PHI to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII and PHI.

104. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII and PHI.

105. Defendant's failure to implement adequate measures to protect the PII and PHI of Plaintiff and Class members violated the purpose of the agreement between the parties.

106. Defendant further failed to adequately and promptly notify Plaintiff and Class members that their PII and PHI had been compromised.

107. Defendant's notice itself is deficient for lack of warning to Plaintiff and Class members that their PII and PHI may have been compromised, and despite "determining that [Plaintiff's] information was impacted" on June 28, 2023, Defendant waited an additional month before notifying Plaintiff.

108. Instead of spending adequate financial resources to safeguard Plaintiff's and Class members' PII and PHI, which Plaintiff and Class members were required to provide to Defendant,

Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class members.

109. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered damages as described in detail above.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

110. Plaintiff incorporates the above allegations as if fully set forth herein.

111. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

112. Plaintiff conferred a benefit upon Defendant by using Defendant's services.

113. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Class members. Defendant also benefited from the receipt of Plaintiff's PII and PHIas this was used for Defendant administer its services to Plaintiff and the Class.

114. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's services because Defendant failed to adequately protect his PII. Plaintiff and the proposed Class would not have provided their PII and PHI to Defendant or utilized its services had they known Defendant would not adequately protect their PII and PHI.

115. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

[INTENTIONALLY BLANK – CONTINUES NEXT PAGE]

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: September 5, 2023

TEWKSBURY & KERFELD, P.A.

By: */s/ Nathaniel J. Weimer*
Nathaniel J. Weimer
88 South 10th Street, Suite 300
Minneapolis, MN 55403
Telephone: (612) 334-3399
Email: nweimer@tkz.com

Mark S. Reich*
Courtney Maccarone*
Gary S. Ishimoto*
LEVI & KORSINSKY, LLP
55 Broadway, 4th Floor, Suite 427
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com
Email: gishimoto@zlk.com

Counsel for Plaintiff

**pro hac vice* forthcoming